Zero Trust Cybersecurity for Industry Control Systems

Industry Control System (ICS) environments often control critical infrastructure such as healthcare, power plants, water treatment facilities, transportation systems, etc. The traditional perimeter-based security approach for ICS assumes devices and network traffic on the inside networks are generally trusted. However, there are three basic threat vectors for the network settings.

1) A user's credentials may have been compromised and used in an attack to gain access to the inside network;

2) A device may be compromised by installing a malware program. That compromised device can then attack other devices on the internal network;

3) A vulnerability can be exploited by adversaries, and that can negatively impact on the internal network.

Zero trust security strategy "Never trust, always verify" changes ICS security from traditional perimeter-based security approaches to a more dynamic and adaptive model based on continuous verification and least privilege access. Zero trust replaces implicit trust with explicit and continuous monitoring and verification based on the risk factors and the threat landscape, regardless of user location or used device. Zero trust reduces the attack surface and minimises the impact of breaches by enforcing strict access controls and segmentation, making it more difficult for attackers to move laterally within the network and access critical systems. Zero trust cybersecurity helps protect ICS systems from cyber threats by ensuring that only authorised users and devices can access and manipulate them.

Industrial Doctorate students in SIT will conduct applied and impactful research with industry, e.g., A Zero Trust Healthcare Monitoring and Securing Framework to be adopted by hospitals to secure remote monitoring and systems management of healthcare devices, systems and network.

Selected Publications:

1. Huaqun Guo and Xingjie Yu. A Survey on Blockchain Technology and its security. Blockchain: Research and Applications, Elsevier, Volume 3, Issue 2, June 2022. (Best Paper Award) Impact factor: 6.9
2. Eyasu Getahun Chekole, Sudipta Chattopadhyay, Martin Ochoa, Huaqun Guo, and Unnikrishnan Cheramangalath. CIMA: Compiler-Enforced Resilience Against Memory Safety Attacks in Cyber-Physical Systems. Computers & Security, Elsevier, Volume 94, July 2020. Impact factor: 5.6
3. Luying Zhou, Huaqun Guo, and Gelei Deng. A fog computing based approach to DDoS mitigation in IIoT systems. Computers & Security - Journal, Elsevier, Vol. 85, pp. 51-62, August 2019. Impact factor: 5.6
4. Dong Li, Huaqun Guo, Jianying Zhou, Luying Zhou, and Jun Wen Wong. SCADAWall: A CPI-Enabled Firewall Model for SCADA Security. Computers & Security Journal, Elsevier, Vol. 80, pp. 134-154, January 2019. Impact factor: 5.6
5. Huaqun Guo, Yongdong Wu, Feng Bao, Hongmei Chen and Maode Ma. UBAPV2G: A Unique Batch Authentication Protocol for Vehicle-to-Grid Communications. IEEE Transactions on Smart Grid, Vol. 2, No. 4, pp. 707-714, December 2011. (No Impact factor in 2011. Now Impact Factor: 8.6)